UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/894,919	06/29/2001	Robert Bruce Hirsh	06975-200001/ Security 13	4606

26171 7590 07/26/2006

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/894,919	HIRSH, ROBERT BRUCE	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20,21,24-28,30-39 and 55-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20,21,24-28,30-39 and 55-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed May 12, 2006, have been fully considered.

2. Claims 20-21, 24-28, 30-39, and 55-95 are pending and have been examined.

Claims 1-19, 22-23, 29, and 40-54 are cancelled.

Response to Arguments

3. In view of the appeal brief filed on 5/12/06, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- **(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,**
- **(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.**

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Response to Amendment

4. Regarding problem 1, Examiner respectfully submits that Cohen et al. (US Patent 6,178,511, hereinafter Cohen) describes not only a single sign-on framework that **enables a user to sign on to multiple target systems and applications** (column 2, lines 60-67, column 3, lines 1-30) (emphasis added) but also suggests using Kerberos in his system (column 9, lines 15-55). As Stevens (NPL Unix Network Programming, Kerberos) teaches, Kerberos provides the argued points (pages 5-7 of the brief) of a client leveraging a connection with an intermediary to access a secured service (claim 67).

5. Regarding problem 2, Examiner points Applicant's attention to **Menezes** et al. (NPL Handbook of Applied Cryptography, chapter 10, page 400, submitted 8/17/05, hereinafter Menezes), **Cohen** (background of the invention), and **Sadovsky** (US Patent 5,689,638, background of the invention) as evidence that the use of client-server communications independent of an intermediary was conventional and well known.

6. Regarding problem 3, Examiner respectfully submits that the suggestion to combine and modify Cohen is found in Cohen (column 9, lines 15-55).

7. Furthermore, Cohen assumes the client accessing a secured service is not trusted, thus the required authentication, further authenticating an intermediary performing tasks for a client would have been obvious to one of ordinary skill in the art.

8. The applicant has not adequately traversed the examiner's use of official notice with regards to the claimed limitations found in claims 35-37, 55-56, 66, 73, 79-81, 84, 87-90, and 95 these features are taken by the examiner to be admitted

prior art since the applicant has not adequately challenged the examiner's use of official notice (see MPEP 2144.03(c), 2144.04).

Claim Objections

9. Claim 24 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 20 already states that the client access is after the intermediary is authenticated.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claim 72 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 72 recites the limitation "constrained information". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 20-21, 24-28, 30-39, and 55-95 are rejected under 35 U.S.C. 103(a) as being unpatentable over Loucks et al. (US Patent 5,481,720, hereinafter Loucks).

Regarding claim 20, Loucks teaches a method, performed by an intermediary, of leveraging a persistent connection with a client to provide the client with access to a secured service, the method comprising:

- receiving a first request from a client at an intermediary, the first request relating to a request for access to the intermediary (abstract, column 8, lines 44-67);
- establishing a persistent connection between the client and the intermediary in response to the first request from the client (figure 6, column 9, lines 1-55);
- receiving a second request from the client at the intermediary, the second request relating to a request for access to a secured service (column 9, lines 1-55);
- and enabling access to the secured service (column 11, lines 6-67).

Loucks does not expressly disclose authenticating the intermediary to the secured service or enabling access by the client based on that. However, Loucks teaches providing secure communications (columns 8-13), suggests communication between the service and the authentication agent, and between the requestor and the authentication agent (column 11, lines 1-67), and authenticating by a secured service a client based on the credentials given to a client by a Kerberos server (column 13, lines 1-46). Therefore, it would have been obvious to one of ordinary skill in the art to also authenticate the entity that gave the credentials to the client, prior to granting access to the client. One of ordinary skill in the art would have been motivated to perform such a

modification to authenticate transactions occurring within network (Loucks, column 13, lines 25-67).

Regarding claim 67, Loucks teaches a method, performed by a client, of leveraging a connection with an intermediary to access a secured service, the method comprising:

- receiving a user request for access to a secured service;
- submitting, by the client, a request, which is based on the user request for access to a secured service, to an intermediary that is physically distinct of the secured service (abstract, column 8, lines 44-67);
- submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary (column 9, lines 1-55, column 11, lines 6-67).

Loucks does not expressly disclose receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request. However, Loucks teaches providing secure communications (columns 8-13), suggests communication between the service and the authentication agent, and between the requestor and the authentication agent (column 11, lines 1-67), and authenticating by a secured service a client based on the credentials given to a client by a Kerberos server (column 13, lines 1-46). Therefore, it would have been obvious to one of ordinary skill in the art to also authenticate the entity

that gave the credentials to the client, prior to granting access to the client. One of ordinary skill in the art would have been motivated to perform such a modification to authenticate transactions occurring within network (Loucks, column 13, lines 25-67).

Regarding claim 81, Loucks teaches a method, performed by a secured service, of allowing a client access based on an authenticated connection between the client and an intermediary, the method comprising (abstract, column 8, lines 44-67):

- receiving, at a secured service, notification of a request by a client to access the secured service (abstract, column 8, lines 44-67);
- conditioned on the existence of a trusted relationship between the secured service and the intermediary, enabling access by the client to the secured service (column 9, lines 1-55, column 11, lines 6-67).

Loucks does not expressly disclose receiving, at a secured service and from an intermediary; or determining whether a trusted relationship exists between the secured service and the intermediary, responsive to the client request. However, Loucks teaches providing secure communications (columns 8-13), suggests communication between the service and the authentication agent, and between the requestor and the authentication agent (column 11, lines 1-67), and authenticating by a secured service a client based on the credentials given to a client by a Kerberos server (column 13, lines 1-46). Therefore, it would have been obvious to one of ordinary skill in the art to also authenticate the entity that gave the credentials to the client, prior to granting access to the client. One of ordinary skill in the art would have been motivated to perform such a

modification to authenticate transactions occurring within network (Loucks, column 13, lines 25-67).

Regarding claim 21, Loucks teaches establishing the persistent connection with the client includes authenticating the client to the intermediary based on keystone authentication information provided by the client (abstract, column 12, lines 1-39). Loucks teaches does not expressly disclose how the intermediary is authenticated, but it would have been obvious to use any authentication method provided by Loucks for the client-secured service connection.

Regarding claim 24, Loucks teaches wherein the intermediary is authenticated to the secured service before the client is enabled access to the secured service (column 11, lines 6-67).

Regarding claim 25, Loucks teaches wherein establishing the persistent connection comprises: receiving keystone authentication information from the client; authenticating the client based on the keystone authentication information to provide a keystone authentication associated with the persistent connection; and establishing the persistent connection with the client based on the keystone authentication (column 11, lines 30-67).

Regarding claim 26, Loucks teaches wherein the second request from the client for connection to the secured service is received after the persistent connection to the client is established (column 12, lines 1-39).

Regarding claim 27, Loucks teaches wherein authenticating the client to the secured service includes: providing a leveraged authentication based on the keystone

authentication associated with the persistent connection; and using the leveraged authentication to establish a connection with the secured service (column 12, lines 1-39). Same reasoning as applied to claim 20 applies.

Regarding claim 28, Loucks teaches wherein the keystone authentication is used to provide the leveraged authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection (column 12, lines 1-39).

Regarding claim 30, Loucks teaches wherein the intermediary comprises a persistent connection service that establishes the persistent connection with the client (column 8, lines 1-55) and a broker service that authenticates the client to the secured service, and authenticating the client includes the broker service receiving from the persistent connection service at a connection request address a communication based on the second request from the client and wherein the connection request address varies systematically with time (column 9, lines 1-55). Same reasoning as applied to claim 20 applies for authenticating the intermediary.

Regarding claim 31, Loucks teaches wherein authenticating the client to the secured service comprises: determining authorization information based on the second request from the client; communicating, to the secured service, an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information; receiving a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service; and enabling the client

to present the authorization information to the secured service to establish the connection with the secured service (columns 12, lines 1-39). Same reasoning as applied to claim 20 applies.

Regarding claim 32, Loucks teaches wherein authenticating the client to the secured service comprises: communicating, to the secured service, an indication that the client desires to connect to the secured service; receiving a response from the secured service indicating that the secured service may accept a connection from the client, wherein the response includes authorization information; and communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service (columns 12, lines 1-39). Same reasoning as applied to claim 20 applies.

Regarding claim 33, Loucks teaches wherein the authorization information is determined by the secured service (columns 12, lines 1-39).

Regarding claim 34, Loucks teaches authenticating the intermediary to the secured service comprises communicating with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service; the authorization information comprises constraint information; and the authorization information may be ineffective to establish a connection with the secured service if one or more connection constraints indicated by the constraint information are not satisfied (columns 12, lines 1-39). Same reasoning as applied to claim 20 applies.

Regarding claims 35-37, Loucks does not expressly disclose these features. However, these features have been admitted per applicant to have been conventional and well known to access control systems at the time the invention was made.

Regarding claim 38, Loucks teaches wherein the connection constraints include a constraint that the authorization information be used within a predetermined time window (Kerberos, column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 39, Loucks teaches wherein the connection constraints include a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered (column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 56, Loucks teaches wherein enabling the client to access the secured service comprises enabling the client to leverage a connection other than the persistent connection established between the client and the intermediary (column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 57, Loucks teaches wherein enabling the client to access the secured service comprises providing constrained authentication information to the client (column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 58, Loucks teaches wherein the constrained authentication information is provided to the intermediary by the secured service (column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 59, Loucks teaches wherein the constrained authentication information is determined by the intermediary and authenticated by the secured service (column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 63, Loucks does not expressly disclose wherein the intermediary is authenticated to the secured service as a consequence of the second request. However, Loucks expressly disclose providing secure communications, therefore it would have been obvious to authenticate each party involved in the process.

Regarding claim 64, Loucks teaches wherein the request for access to the secured service comprises an explicit request for access by the client (column 12, lines 1-67).

Regarding claim 65, Loucks teaches wherein the request for access to the secured service comprises a client communication received via the secured service (column 12, lines 1-67).

Regarding claim 66, Loucks teaches wherein the secured service is available for direct authentication by a user without establishing a persistent connection between the user and the intermediary (Kerberos).

Regarding claim 68, Loucks teaches wherein establishing the authenticated connection between the client and the intermediary comprises: sending, by the client, keystone authentication information to the intermediary; and receiving, from the intermediary, verification of the keystone authentication information (column 11, lines 30-67).

Regarding claim 69, Loucks teaches wherein submitting the request to the intermediary for access to the secured service prompts the intermediary to authenticate itself to the secured service without provision by the client of authentication information duplicative or additional to the keystone information (column 11, lines 30-67). Same reasoning as applied to claim 67 applies for authenticating the intermediary.

Regarding claim 70, Loucks does not expressly disclose authenticating the intermediary. However, Loucks teaches wherein the client is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication. Therefore, it would have been obvious to also authenticate the intermediary.

Regarding claim 71, Loucks does not expressly disclose wherein the constrained authorization information has been issued by the secured service and sent by the secured service to the intermediary. However, Loucks teaches wherein the client is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication and the constrained authorization information under Kerberos is issued using information regarding the secured service. Therefore, it would have been obvious to have the secured service send constrained authorization information to the intermediary in the same way the intermediary sends constrained information to the client.

Regarding claim 72, Loucks teaches wherein the constrained information has been provided by the intermediary and authenticated by the secured service (column 4, lines 40-67, column 5, lines 1-30).

Regarding claims 60, 74, and 92, Loucks teaches wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel (column 8, lines 1-35).

Regarding claims 61, 75, and 93, Loucks teaches wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service (column 8).

Regarding claims 62, 76, and 94, Loucks teaches wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service (column 8, lines 1-35).

Regarding claim 77, Loucks teaches wherein the client request for access to the secured service comprises an explicit request for access by the client (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 78, Loucks teaches wherein the client request for access to the secured service comprises a communication sent by the client to the intermediary via the secured service (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 79, Loucks teaches wherein the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary (columns 3-4).

Regarding claim 80, Loucks teaches wherein the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 82, Loucks teaches wherein enabling access by the client comprises issuing constrained authorization information to the intermediary for use by the client to access the secured service (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 83, Loucks teaches wherein enabling access by the client further comprises receiving the constrained authorization information from the client (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 85, Loucks teaches wherein enabling access by the client comprises authenticating constrained authorization information to be provided by the intermediary to the client to access the secured service (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 86, Loucks teaches wherein enabling access by the client further comprises receiving the constrained authorization information from the client (column 11, lines 30-67, column 12, lines 1-30).

Regarding claims 73, 84, and 87, Loucks teaches wherein the constrained authorization information comprises one or more of a constraint that the authorization information has been used no more than a predetermined number of times (see rejection of claims 35-37), a constraint that the authorization information be used within a predetermined time (Kerberos, column 4, lines 40-67, column 5, lines 1-30), and a

constraint that the authorization information be received from only the client (column 4, lines 40-67, column 5, lines 1-30).

Regarding claims 55 and 88, Loucks teaches wherein enabling access by the client to the secured service comprises enabling the client to access the secured service independent of the intermediary (column 4, lines 40-67, column 5, lines 1-30).

Regarding claim 89, Loucks teaches wherein the connection between the client and the secured service is established by the client leveraging a connection other than a connection between the client and the intermediary (column 11, lines 30-67, column 12, lines 1-30).

Regarding claim 90, Loucks teaches wherein determining whether a trusted relationship exists between the secured service and the intermediary comprises receiving authentication information from the intermediary (column 11, lines 1-67).

Regarding claim 91, Loucks teaches wherein the intermediary provides the authentication information to the secured service without provision by the client of other authentication information that is duplicative or additional to keystone authentication information provided by the client to the intermediary to establish the authenticated connection between the client and the intermediary (column 11, lines 1-67). Same reasoning as applied to claim 81 applies for authenticating the intermediary.

Regarding claim 95, Loucks teaches wherein the secured service is available for direct authentication by a user without determining whether a trusted relationship exists between the secured service and the intermediary (columns 3-4).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Dare et al. (US patent 5,684,950) teaches an intermediary for brokering connections between a client and a server (abstract). Fortinsky (US Patent 5,815,574) teaches secure access to external resources, a client receiving a ticket from a server to access another server (abstract). Krajewski, Jr. et al. (US Patent 5,590,199) teaches authenticating users to a trusted agent and receiving a ticket for access other resources (abstract, summary). Haverinen (US Patent Application Publication) teaches using Kerberos and authenticating the tickets (abstract).

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

16. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

17. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC 7/21/06